

## **Exhibit D**

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS**

ALLIANCE FOR AUTOMOTIVE  
INNOVATION,

Plaintiff,

v.

MAURA HEALEY, ATTORNEY GENERAL  
OF THE COMMONWEALTH OF  
MASSACHUSETTS, in her official capacity,

Defendant.

Civil Action No. 1:20-cv-12090

**DEFENDANT'S TRIAL AFFIDAVIT OF BRIAN ROMANSKY**

I, Brian Romansky, declare and say as follows:

**I. Professional Qualifications**

1. I have been retained as an expert by counsel for the defendant Attorney General in the above captioned litigation. I have 27 years of experience in advanced security technology research and innovation spanning automotive, healthcare, financial services, defense, and industrial applications. I have expertise in, among other issues, cybersecurity best practices; Public Key Infrastructure (PKI); operational technology networks and critical infrastructure networks; and vehicle-to-vehicle messaging. A true and accurate copy of my curriculum vitae is marked as Exhibit 520 and is attached hereto.

2. I am currently employed as the Chief Innovation Officer of Owl Cyber Defense, a cybersecurity technology company that serves national defense, government intelligence, and commercial critical infrastructure customers. Formerly, I was a Senior Director of Strategic Technology at Escrypt Embedded Security, a division of the automotive component

manufacturer Robert Bosch LLC, where I was responsible for technology strategy related to connected vehicle security. In that role, I worked with leading automotive manufacturers to define and implement methods of securely connecting vehicles to trusted external applications in other vehicles as well as roadside equipment and other trusted devices. While at Escrypt and in a prior role as VP of Strategic Technology at TrustPoint Innovation, for a time spanning 2015 through 2018, I served as a technology advisor to the Crash Avoidance Metrics Partners LLC (CAMP), a pre-competitive research organization that was contracted by the United States Department of Transportation (DOT) to study, define, and validate the Security Credential Management System (SCMS), which is an advanced PKI designed to support the nation wide deployment of secure Connected Vehicle messaging.

3. In my career, I have worked extensively with automotive vehicle systems, CAN bus messages, network architecture, and related cybersecurity systems. For example, I have worked with manufacturers in the development of in-vehicle intrusion detection and reporting solution. I have written software to implement vehicle-to-vehicle messaging for collision avoidance. I was the program and product manager for the development of software designed to run in a vehicle and interact directly with multiple in-vehicle systems. I have participated in plug-fests where device authentication and direct vehicle-to-vehicle messages have been tested. I have visited multiple state DOT connected vehicle pilot sites as well as planned and executed connected vehicle demonstrations. I have experience with systems that use secure boot, secure software validation, and secure software updates.

4. I am being compensated by the Office of the Attorney General at the rate of \$350 per hour for my work on this case.

## **II. Overview**

5. The 2020 Massachusetts Right to Repair Law consists of two primary requirements. First, Section 2 of the law requires that “motor vehicle owners’ and independent repair facilities’ access to vehicle on-board diagnostic systems shall be standardized and not require any authorization by the manufacturer, directly or indirectly, unless the authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer.” Second, Section 3 requires vehicles equipped with a telematics system to include “an inter-operable, standardized and open access platform across all of the manufacturer’s makes and models,” which “shall be capable of securely communicating all mechanical data emanating directly from the motor vehicle.” The law does not specify what technology must be used to enable the platform.

6. Based on my experience with automotive networks, authentication technology, and broader cybersecurity best practices, it is my opinion that the access required by the 2020 Right to Repair Law can be achieved without compromising the security and integrity of vehicle networks, and thus maintaining driver safety. Specifically, Section 2 of the 2020 Right to Repair Law does not require vehicle manufacturers (OEMs) to limit their ability to stop unauthorized third parties from accessing data in the vehicle. Through the use of PKI technology, it is feasible for the OEMs to remove themselves from the authorization process for access to vehicle onboard diagnostic systems while still keeping their vehicles secure against attacks by unauthorized users.

7. In addition, there are multiple ways that the OEMs could comply with Section 3 of the 2020 Right to Repair Law without compromising the security of their vehicles. One

option to comply with Section 3 of the 2020 Right to Repair Law is to employ the Secure Vehicle Interface (SVI) standards. The SVI standards can be implemented in software on multiple types of hardware platforms (wired and wireless) to comply with the requirements of the 2020 Right to Repair Law. My opinion provides an overview of these standards and their development, as well as how their use in conjunction with whatever hardware implementation an OEM chooses enables compliance with Section 3 without introducing significant new cybersecurity risks. Vehicle networks that follow design guidelines and recommended architectures from National Institute of Standards and Technology (NIST), SAE International (SAE), and even the National Highway Transportation Safety Administration (NHTSA) cybersecurity guidelines will be well positioned to implement the targeted access control and authentication required to safely allow third-party access to the diagnostic and repair functions identified by the Massachusetts law.

8. I am aware that there are some vehicles that already take advantage of an authorization solution that could be extended to cover access as defined by the new 2020 Right to Repair Law. These vehicles could potentially extend the same authorization solution to allow selective telematic access to systems within the vehicle for diagnosis and repair functions. For vehicles with older, legacy designs (specifically, older designs that do not support advanced authorization for diagnostic tools), there are existing after-market solutions that can be adapted by OEMs without requiring any design changes to the vehicle network and may achieve compliance with the new law.

### **III. Overview of Cybersecurity Best Practices**

9. The plaintiff's retained experts Daniel Garrie and Bryson Bort have erroneously opined that OEMs cannot comply with the requirements of the 2020 Right to Repair Law

without introducing cybersecurity risks that could compromise a vehicle's critical systems and emissions controls. To meaningfully evaluate whether compliance with the 2020 Right to Repair Law is feasible without introducing cybersecurity risks that could compromise vehicle systems, I first provide an overview of cybersecurity best practices in the automotive industry.

10. Effective cybersecurity can only be achieved through the coordinated application of a broad set of techniques and mechanisms. While most attention is typically drawn toward specific enforcement controls like firewalls and gateways, there is no single feature or function that can assure security in a complex system such as a modern automotive network. Most cybersecurity best practices focus on mundane activities such as estimating risk, documenting requirements, and creating and executing an implementation plan. When these practices are followed, the resulting systems are not only resilient to threats, they are also well positioned to safely support new access control features, such as the requirements of the 2020 Right to Repair Law.

11. The NIST Cybersecurity Framework describes the breadth of activities and skills that are required to design, develop, and maintain a secure system. Throughout the framework there is a strong emphasis on estimating risk, defining clear requirements, and documenting design decisions. The framework is divided into five functions:

Identify: Identify known threats in the design stage.

Protect: Protect against known threats with effective countermeasures.

Detect: Detect suspicious activity in a system after it is deployed — this may be a sign of a new threat that was not identified in the original design.

Respond: Respond to suspicious activity by applying appropriate countermeasures or through notification and logging.

Recover: Define a recovery plan to update or replace systems after a compromise has been detected.

12. A similar emphasis is prescribed in the latest draft of the ISO/SAE 21434 Cybersecurity Engineering standard for Road Vehicles. *See* SAE International, Surface Vehicle Standard, “Road Vehicles - Cybersecurity Engineering,” ISO/SAE DIS 21434, Issued 2020-02-12. This draft is currently in the “Approval” stage, which is the last step prior to “Publication” according to the ISO process. The bulk of this standard describes organizational and team structures as well as risk assessment methodologies that should be used to produce a secure system. The latest draft revision of the NHTSA Cybersecurity Best Practices for Modern Vehicles relies heavily on the new ISO/SAE 21434 specification and reflects the same design principles. *See* U.S. Department of Transportation NHTSA, “Cybersecurity Best Practices for the Safety of Modern Vehicles,” Draft 2020 Update.

13. Vehicle networks that have been designed and maintained in alignment with NIST, ISO/SAE 21434, and NHTSA cybersecurity best practices will rely on robust security mechanisms with clearly documented assumptions and threat analysis. Such systems contain layers of protection, also known as “defense-in-depth,” such that a breach at one point does not expose the entire network. Modern vehicles that have these properties are well suited to fully implement the 2020 Right to Repair Law.

14. One specific technique that OEMs may use to protect vehicle networks is the use of network segmentation and intelligent gateways between network segments. These gateways act as sophisticated firewalls that enforce segmentation between different subsystems within a vehicle network. A gateway can interpret commands and route them based on a strict security policy that can account for multiple factors such as the source and destination systems, the current vehicle state, and detailed protocol analysis to validate the integrity of individual messages. This type of intelligent gateway is used to selectively and

safely route valid messages, including diagnostic and repair requests, across network boundaries. These gateways are capable of permitting only valid diagnostic and repair requests across network boundaries and preventing improper requests that could damage a vehicle from traveling across network boundaries to critical systems. Some vehicles that offer telematic-enabled diagnostic capabilities through their dealership partners already have this type of gateway technology built-in to their vehicles. That is how they are able to move diagnostic messages from safety critical systems such as brakes and steering out through the existing telematic radio interface.

15. Another specific technique that OEMs may use to protect vehicle networks is vehicle condition checks—sometimes called “rationality” checks—that are performed within existing vehicle computers or electronic control units (ECUs). Modern software in these systems is designed to confirm that the vehicle is in a safe state prior to allowing diagnostic or repair procedures that could potentially interfere with driver safety. For example, an anti-lock brake system may enable a diagnostic procedure only when the vehicle is parked and stationary with the engine off. This type of safety check is specifically recommended in the 2020 draft NHTSA Cybersecurity Best Practices in technical recommendations T.5 and T.6:

*[T.5] Diagnostic features should be limited, as much as possible, to a specific mode of vehicle operation which accomplishes the intended purpose of the associated feature.*

*[T.6] Diagnostic operations should be designed to eliminate or minimize potentially dangerous ramifications if they were misused or abused outside of their intended purposes.*

16. This type of practical, built-in safety enforcement mechanism is fully compatible with the 2020 Right to Repair Law’s access requirements. The 2020 Right to Repair Law does not require that these mechanisms be removed or disabled. In fact, due to

this level of defense-in-depth that is built into many vehicles, compliance with the 2020 Right to Repair Law is feasible, practical, and safe.

17. The NHTSA best practices clearly recognize and encourage the need to enable diagnostic and repair capabilities for all technicians. For example, guideline G.43 states:

*[G.43] The automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by alternative third-party repair services authorized by the vehicle owner.*

The same section advises that “cybersecurity should not become a reason to justify limiting serviceability.” As such, full compliance with the NHTSA best practice guidelines would harmonize cybersecurity and serviceability, and is directly aligned with the requirements of the 2020 Right to Repair Law.

18. It is noteworthy that none of the best practice guidelines place an emphasis on the use of obscure or proprietary mechanisms to protect vulnerable networks. In fact, they explicitly recommend the use of mature, standards-compliant mechanisms as well as clearly documented assumptions and protocols. This is a significant break from the past where some OEMs attempted to develop their own proprietary security technologies that relied on secrecy of the design details to protect the infrastructure. This approach, sometimes called “security by obscurity,” is an ineffective way to protect vehicle networks and has historically led to a number of breaches. Security researcher Bruce Schneier stressed this point when he wrote, “the argument that secrecy is good for security is naïve.” Schneier, Bruce, “The Nonsecurity of Secrecy,” *Communications of the ACM*, October 2004, Vol. 47 No. 10, at 120.

#### **IV. Section 2 of the 2020 Right to Repair Law**

19. Section 2 of the 2020 Right to Repair Law expands on the preexisting law by adding the following language:

*vehicle owners' and independent repair facilities' access to vehicle on-board diagnostic systems shall be standardized and not require any authorization by the manufacturer, directly or indirectly, unless the authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer.*

In this section of my opinion, I focus on the final clause of the new language, and conclude that it is feasible for automobile manufacturers to implement an “*authorization system for access to vehicle networks and their on-board diagnostic systems that is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer.*”

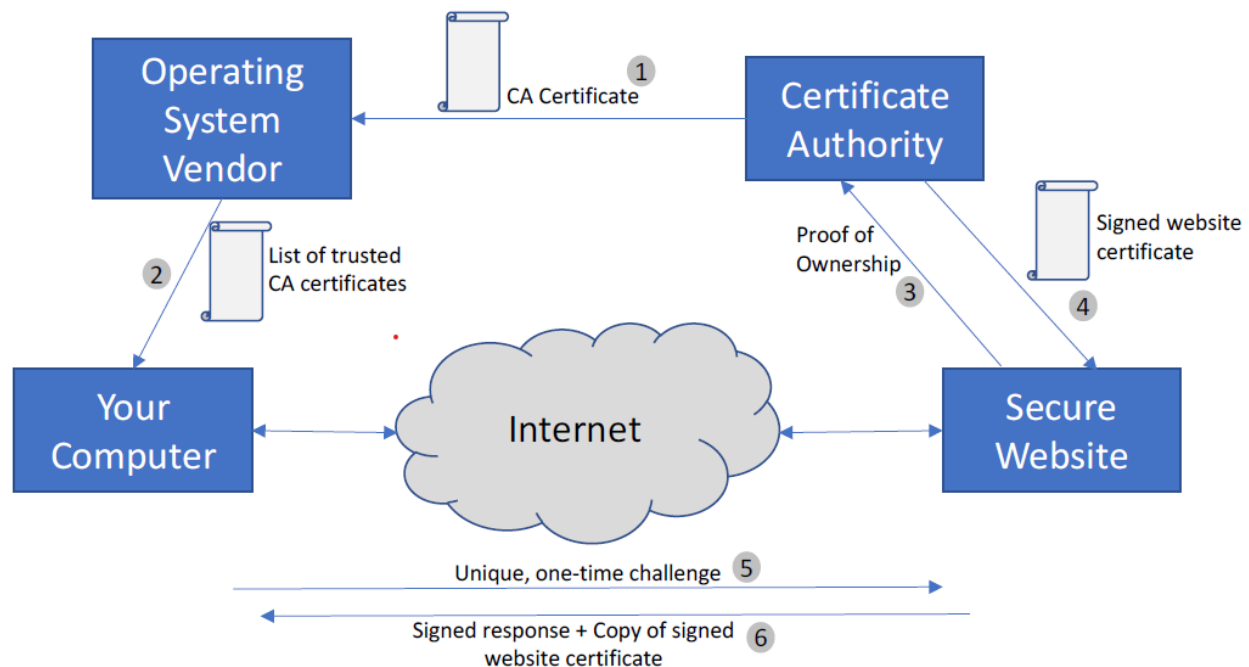
**A. Authentication and Authorization Technology**

20. In computer networks, including connected vehicles, authentication and authorization are terms used to describe the process of validating the identity and authentic access rights of a remote user or system. For example, when a repair technician uses a scan tool to read or write to an ECU within a vehicle, the vehicle network can optionally require that the technician or the scan tool prove that they have the correct access rights to interact with the vehicle. In some systems, the level of permission granted to a specific operator or tool can be very narrowly defined, such that the tool only has access to a specific control unit or only has permission to execute a small set of commands for a limited time. This detailed level of authorization is often referred to as “fine-grain access control” or is sometimes defined as Role-Based Access Control (RBAC).

21. The simplest and most obvious method of authentication is a classic username and password combination. The theory behind this basic approach is that a system or person who has knowledge of a presumably secret password must be the person who they claim to be.

22. Sophisticated authentication systems typically rely on certificate-based authentication that is enabled by Public Key Infrastructure (PKI). You can see the benefit of a PKI every time you visit a secure website on the internet: The “lock” symbol displayed by most modern web browsers is a confirmation that the browser software has been able to validate the identity of the website’s server, a validation that is made possible by PKI.

23. Using the example of a secure website on the internet, Figure 1 shows a simplified model of the key infrastructure and the flow of messages associated with PKI.



*Figure 1: Simplified PKI message flow for a secure website.*

24. In general, in step 1 the Certificate Authority (CA) registers with an operating system vendor (such as Microsoft for Windows) by securely delivering a public certificate—a special digital file that contains a copy of the CA’s “public key,” which is needed to verify any

future digital signatures produced by the CA. Importantly, the CA for any given PKI can be operated by an independent entity, sometimes called a “trusted third party.”

25. In step 2, a copy of this public certificate is bundled with the operating system that you, as a user, will install on your computer. These steps (1 and 2) happen when a new CA is established. The leading operating system vendors are very rigorous in ensuring that only trusted CAs are included in their systems. As a result, there is a relatively short list of trusted CAs and they are not updated very often.

26. Then, a new website is created and its operator desires to enable it to support secure sessions. In step 3, the website operator chooses a CA vendor and provides proof that the operator is the rightful owner of the website and that it has direct control over the server that will host the website. Once this is done, the CA issues the operator a special certificate that proves ownership of the site, which is delivered back to the website operator in step 4. The site operator installs this file on the website’s server. These steps are done when the new secure website is established (and it is repeated prior to the expiration period of the certificate).

27. Finally, in Steps 5 and 6, you, as an ordinary user, choose to visit the secure website. In order to establish a secure session between your computer and the website’s server, your web browser sends a “challenge” to the server. The website’s server then responds to that challenge with a digital signature, along with a copy of the certificate that was issued by the CA to the website operator when the site was created. Your computer validates the signature on the challenge response, thereby verifying that the website’s server is indeed the system with which you are communicating. Your computer also verifies that the website’s certificate is valid and confirms that the CA is included in the trusted list provided by the

operating system. If all of these checks look good, then the web browser will show the green “lock” symbol indicating that it has validated that the website’s server is a valid system that is managed by a known or trusted operator. These steps are repeated every time a user or system establishes a new secure connection.

**B. One Method of Compliance with Section 2: A Public Key Infrastructure Administered by an Entity Unaffiliated with a Manufacturer**

28. This same technology can be readily adapted to allow modern vehicles to reliably authenticate trusted diagnostic tools used by independent technicians. Vehicles that fully comply with the 2020 Right to Repair Law will need to support authentication and authorization of a broad array of different users and diagnostic tools. Fortunately, many modern vehicle networks already support sophisticated algorithms to enable authentication and fine-grain access controls. Extension of these controls to include independent repair shops may be as simple as providing a software update or extending an existing agreement with an authentication service provider.

29. An example of this can be seen in the operation of the AutoAuth® Authentication Authority. Use of this new web-based registration service is required in order to connect service and diagnostic tools to new vehicles made by FCA that include a Secure Gateway Module (SGW). This service allows independent repair facilities to register security-enabled diagnostic tools through the AutoAuth® web portal so that they can be authenticated by the SGW module in FCA vehicles. The Tools Vendor Agreement (<https://info.autoauth.com/wp-content/uploads/2021/02/ISS-AutoAuth-Tools-Vendor-Agreement-02-10-2021.pdf>) for this service states that it is operated by INTEGRITY Security Services, Inc. Based on INTEGRITY’s experience in developing and running certificate services (<https://www.ghsiss.com/certificate-services/>), it is likely that a PKI mechanism is

powering this wide-scale capability. In this case, the independent operator of the AutoAuth® platform is acting as a trusted third-party that operates the CA, and thus enables SGW-enabled vehicles to trust requests from registered diagnostic tools.

30. One of the benefits of this approach is that it can operate at a very large scale. After a one-time registration, the actual authentication between the diagnostic tool and the SGW module does not require a live connection to the AutoAuth® CA server. This means that an unlimited number of vehicles and tools can utilize the mechanism without requiring a massive increase in the scale of the AutoAuth® hosted service. Today the SGW appears to only support direct, wired connections to the J-1962 port (*i.e.*, OBD port) in a vehicle. However, the same authentication mechanism can be extended to work through a telematic interface.

31. I believe that this approach meets the requirements of Section 2 of the 2020 Right to Repair Law. This mechanism allows for one or more trusted CA services to be operated independent from any one OEM, such that the authentication process can be fully independent of OEM control.

32. An example of an independent organization that currently provides a similar vetting service for the automotive industry is the National Automotive Services Taskforce (NASTF). One of the roles that this organization has taken on is to provide a vetting service which reviews the background and training of independent repair technicians. This service is trusted by OEMs to authorize approved vendors to access special codes and software needed to reprogram electronic keys and immobilizer components in vehicles. The vetting process applied by NASTF can serve as a model for certificate issuing policies that may be applied when granting certificates to independent repair facilities to enable them to perform key

operations such as calibration of safety systems. It is my opinion that one or more CAs, implementing a common policy and operating independent of any OEM, would provide the level of independence required by the 2020 Right to Repair Law.

**C. Another Method of Compliance with Section 2 of the 2020 Right to Repair Law: Enhanced V2X Administered by an Unaffiliated Entity**

33. Another viable option to support secure authentication for diagnostic tools in compliance with the 2020 Right to Repair Law is to build on the V2X security solution that has been jointly developed by major OEMs in collaboration with the United States Department of Transportation (DOT) and other global regulatory bodies. V2X refers to secure wireless connections between vehicles and any external services. Originally developed for fast Vehicle to Vehicle (V2V) messaging to support collision avoidance, this technology has been extended and validated for use in Vehicle to Infrastructure (V2I) (secure wireless connections between vehicles and roadside equipment) and broader Vehicle to Anything (V2X) messaging.

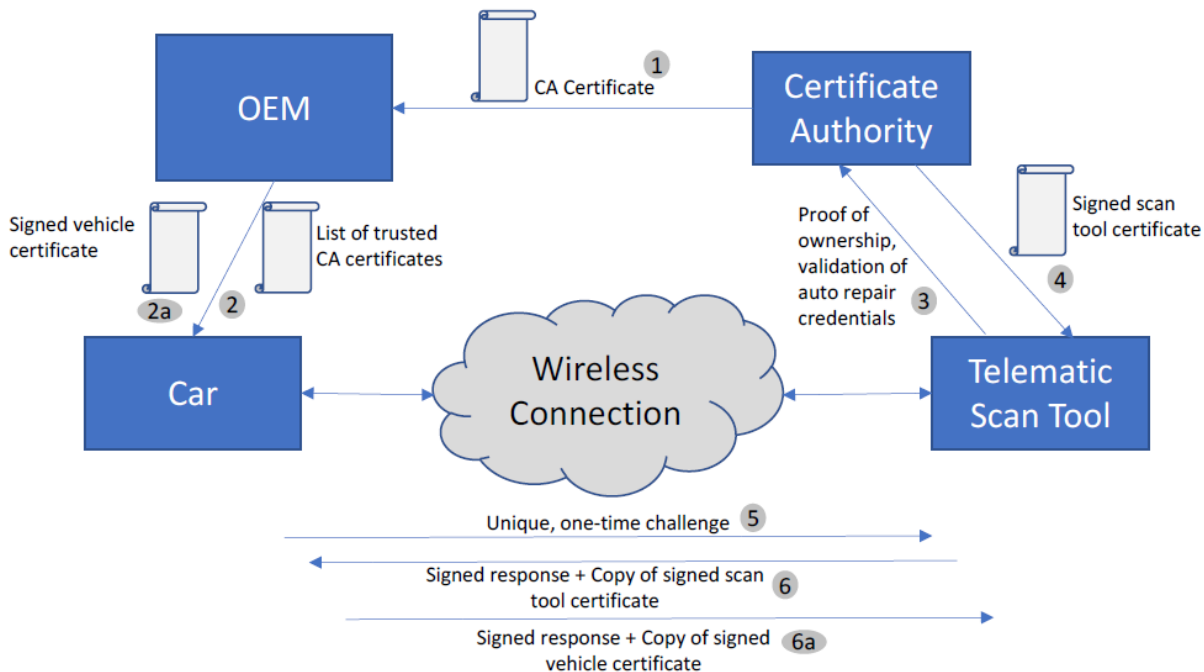
34. As with the previous example, the V2X standards rely on the powerful authentication capabilities of PKI. A key difference is that conventional PKI, like the lock that you see in your web browser or the AutoAuth® service used by FCA, uses a certificate schema called X.509. This schema was initially developed for use in complex financial services transactions, and it has been adapted for the broader internet and other applications. The schema of a certificate defines the way that data is stored in the digital representation of the certificate. In the case of X.509, this includes a complex set of permission fields that can be optionally filled in by the certificate authority. These permissions were intended for use in financial systems and were not designed for use in vehicle networks.

35. V2X technology instead relies on the IEEE 1609.2 certificate type that was specifically designed for use in vehicles. *See* IEEE Vehicular Technology Society, “IEEE Std

1609.2a™-2017,” IEEE, New York, NY. The new certificate schema has several advanced new features such as implicit certificates which allow for much more compact over-the-air messages. It also introduces a mechanism for announcing new services and validating detailed device permissions and access control rights. This means that, when a CA issues a certificate to a trusted device, such as a vehicle diagnostic tool, the CA can assign a set of specific permissions to the device that define what functions it is authorized to perform. These details are extensively documented and clearly defined for specific automotive use cases. This technology has been tested through a series of Connected Vehicle pilot projects that have been documented by the DOT. These pilots have demonstrated that this technology is robust and reliable for use in vehicles.

36. The V2X capability is powered by a new type of certificate authority infrastructure called the Security Credential Management System (SCMS) which is currently supported by the DOT. This infrastructure and authentication capability can be extended to support advanced authentication for vehicle diagnostics and repair. The combination of the efficient 1609.2 certificate format with the validated scalability of the SCMS infrastructure make this approach ideal for diagnostic tool authentication to vehicles.

37. Figure 2 shows a simplified diagram of the transactions required to establish a secure connection between a secure scan tool and a vehicle. This highly simplified diagram shows the parallels with the overall process described for a secure web page in Figure 1.



*Figure 2: Secure connection for a remote scan tool.*

38. In this case, the Certificate Authority (CA) must contact vehicle manufacturers (OEMs) to get the CA's public certificate included in a list of trusted CA certificates that is installed in individual vehicles (steps 1 and 2). Note that, in this case the OEM also installs a certificate that belongs to the vehicle itself (step 2a). This vehicle-specific certificate will be used to prove the identity of the car in a later step.

39. A service operator then registers a new scan tool with one of the trusted CAs by proving their identity, showing that they own and operate the scan tool, and that they are qualified to diagnose and repair vehicles (step 3).

40. Once satisfied, the CA may issue a certificate to the scan tool (step 4). At this point, it is possible for the CA to include a list of specific permissions in the scan tool certificate. For example, a scan tool that is only intended to be used for diagnostics will not be

granted permission to perform software updates or to send other commands to the vehicle.

This provision allows for strict controls to be placed on scan tools to limit their functions to a well-defined set of operations. This mechanism provides a technical implementation of the fine-grain access controls. The permissions granted to a specific tool can be adjusted based on the capabilities and intended use of the tool.

41. Once a scan tool is registered with a trusted CA, it is possible for the vehicle to establish a secure connection with the tool using the sequence shown in steps 5 and 6. In this instance, the vehicle owner may choose which service provider they want to use to diagnose and repair their vehicle. Note that in some cases, the connection request may originate from the scan tool to the vehicle which can be accepted or rejected based on instructions from the owner. The additional step shown as 6a allows the car to prove its authenticity and identity to the scan tool by delivering a digitally signed message and its certificate. This is known as “mutual authentication,” and sometimes referred to as a technical implementation of a “handshake.” In this case the car and the scan tool each end up with proof that they are connected to an authentic and clearly identified device on the other side of the connection. Once the secure connection is established, the scan tool may send diagnostic messages to the vehicle. Each message can be checked against the set of permissions allowed in the scan tool’s certificate to ensure that it is authorized to perform the requested function.

#### **D. Unaffiliated Entity**

42. One of the significant benefits of the use of PKI technology is that the CA which issues credentials can operate independent of the end-entities who are involved in a transaction. In the web browser example, the CA was able to verify ownership of a specific internet web server and convey that ownership information to a consumer using a

commercially supported browser. In this case the CA may receive payment from the web site operator to cover the cost of operating the CA service, but the CA itself operates as an independent company. Many such CA operators exist, enabling nearly all commercial websites to be trusted by nearly all browsers globally.

43. The same approach can be applied to cars. One or more CA operators can issue credentials that can be used by OEMs and tool vendors. There is no need for a single company to emerge to manage these trust relationships. This can be achieved through one or more unaffiliated entities. As previously mentioned, an independent organization that follows a regular, documented process such as NASTF provides an example of how this can operate independent of any one OEM.

**E. Conclusion – OEMs Can Comply with Section 2**

44. The discussion of PKI technology and authentication techniques demonstrates two methods that can be used to implement Section 2 of the 2020 Right to Repair Law. I have described how conventional X.509 certificates can be used for large-scale deployments such as secure websites on the internet. I have also described how more advanced V2X certificates can be used to achieve the same goal. In both cases, the CA operator can be fully independent from the OEM or the repair shop, in compliance with Section 2 of the 2020 Right to Repair Law.

**V. Section 3 of the 2020 Right to Repair Law**

45. Section 3 of the 2020 Right to Repair Law requires only those vehicles equipped with a telematics system to include “an inter-operable, standardized and open access platform across all of the manufacturer’s makes and models,” which “shall be capable of securely communicating all mechanical data emanating directly from the motor vehicle.” The

Secure Vehicle Interface approach provides a detailed, documented, and standards-compliant way to deliver this capability without compromising driver safety or vehicle cybersecurity.

**A. SVI Standards**

46. The Secure Vehicle Interface (SVI) is a technical design pattern that was developed to support an interoperable interface for diagnostic and repair data, in addition to other Intelligent Transportation Systems (ITS) functions. ITS systems refers to a collection of technologies that support transportation and road use. Some examples include traffic light and congestion monitoring systems, road ice warning systems, and collision avoidance technology.

47. The SVI design can support both a direct wired and a wireless telematic connection and provides a path to compliance with the 2020 Right to Repair Law. (The 2020 Right to Repair Law defines “telematics system” as “any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such information . . . utilizing wireless communications to a remote receiving point where it is stored.”)

48. The SVI design is documented in three technical standards published jointly by the European Committee for Standardization (CEN) and the International Organization for Standardization (ISO). CEN is an association that brings together the National Standardization Bodies of 34 European countries. Its technical working groups develop a variety of standards, many that impact technology used on vehicles sold in the EU. CEN has broad participation by technical representatives from nearly all global auto manufacturers. ISO is an independent, non-governmental international organization with a membership of 165 national standards bodies. ISO sets global technical and performance standards including standards for use in

vehicles and, in some cases, votes on and adopts standards created by technical teams in regional standards bodies such as CEN.

49. The SVI specific standards are:

- **CEN/ISO TS21177 – ITS station security services for secure session establishment and authentication between trusted devices**  
Defines the security services used to establish secure sessions and authentication between trusted devices and roles supported by operators using those devices.
- **CEN/ISO TS21185 – Communication profiles for secure connections between trusted devices**  
Specifies a methodology for defining ITS Station communication profiles based on standardized communication protocols to interconnected trusted devices.
- **CEN/ISO TS21184 – Global Transportation Data Management (GTDM) framework**  
Defines the management of messages containing information of sensor and control networks specified in data dictionaries.

50. These standards were developed and grouped together into the SVI set to create a standard and secure interface between cars and technology-enabled tools that support diagnostic and repair operations in vehicles. They are based on mature, commonly used security and network architecture approaches that are well known in the automotive industry. These standards can be used to facilitate and accelerate adoption of an interoperable interface, including a telematics interface, for secure access to vehicle data necessary for diagnostics, maintenance, and repair.

51. TS21177 defines a method of adapting the widely used Transport Layer Security (TLS) mechanism to utilize the IEEE 1609.2 certificate architecture. The IEEE 1609.2 certificate standard was first published on April 26, 2013. As described in paragraphs 35–36, it was initially adopted for use in direct Vehicle to Vehicle (V2V) messaging for collision avoidance. It has subsequently been adopted for extended use in Vehicle to

Infrastructure (V2I), and more general Vehicle to Anything (V2X) applications and incorporated into the ETSI (European Telecommunications Standards Institute) TS103097 standard. The publication of TS21177 has further expanded the applicability of the 1609.2 certificate structure to enable mutually authenticated TLS sessions for secure point to point messaging. This means that when a communications session is established using the TS21177 standard, both the originator of the session and the target system can each validate the authenticity and identity of the other system. Once a TLS session is established, the communicating systems can be confident that they share a secure, secret channel that ensures the confidentiality, integrity, and authenticity of the data that is received through that channel.

52. TS21185 defines a standard set of communication profiles that can be enabled using conventional wireless technologies including WiFi, 4G and 5G cellular, and other common wireless connection methods. As wireless communications technology evolves, this standard assures an interoperable interface in either a wired or wireless form, which assures compatibility with interfaces that utilize both older and newer technologies. This standard directly references the IEEE 802 series of networking standards which define the WiFi network interface. By including this wireless capability through a reference, the TS21185 standard can evolve to adopt future enhancements and improvements that may be made to the WiFi interface over time. It also inherits the extensive work done by the 3rd Generation Partnership Project (3GPP) collection of standards groups. This collection of standards define the physical and logical requirements for several modes of wireless telecommunications typically associated with cellular phones and other wide-area networking technologies. Here too, by referencing existing standards from international organizations, the TS21185

specification can incorporate future enhancements that may be made to the existing 4G and 5G cellular architectures that fall under the 3GPP collection of standards.

53. TS21184 defines a data dictionary, or a way to translate between proprietary, vehicle- specific messages and protocols and a standard, published set of external message types. Rather than ask OEMs to all adopt the same message format for their internal network communications, TS21184 recognizes that vehicles will continue to operate using unique, customized, or proprietary message types. This is a key factor in rapid deployment of an SVI solution. The adoption of the TS21184 data interchange format does not require that OEMs make any change to the internal message formats used within their vehicles. The standard explicitly recommends that a secure gateway module should be used between the internal network and any external SVI device. This secure gateway approach allows for translation of messages as they transition between the external SVI interface (as defined in TS21185) and the internal, OEM-specific message format.

54. Together, TS21184 and TS21185 provide a translation interface between the existing unique, proprietary internal messages and a common external interface that can be easily shared with tool vendors.

## **B. Background on V2X and SCMS**

55. The National Highway Safety Transportation Administration (NHTSA), a division of the DOT, began serious study of the potential for V2V messaging to prevent vehicle collisions as early as 2013. *See* DOT HS 811 733, “Light Vehicle Crash Avoidance Needs and Countermeasure Profiles for Safety Applications Based on Vehicle-to-Vehicle Communications,” OMB No. 0704-0188, April 2013. By 2015, NHTSA was already conducting safety pilot studies with thousands of vehicles and specially equipped Roadside

Units (RSUs) in Ann Arbor Michigan. *See* DOT HS 812 171, “Safety Pilot Model Deployment Test Conductor Team Report,” DTFH61-11-C-00040, June 2015. This research demonstrated the feasibility of equipping vehicles with safety-critical collision avoidance technology based on PKI technology and wireless messaging.

56. To scale up this model to support the need to register and securely manage security credentials for all vehicles on U.S. roads, the DOT supported the development and validation of a Security Credential Management Systems (SCMS) infrastructure. The architecture of the SCMS was independently reviewed by Booz Allen Hamilton in 2013. *See* FHWA-JPO Report, “Security Credentials Management System (SCMS) Design and Analysis for the Connected Vehicle System,” DTFH61-11-D-00019, December 2013. Subsequent publications of the SCMS specification were created by the Crash Avoidance Metrics Partnership (CAMP) as a result of Vehicle Safety Communications 5, a project conducted with direct participation from General Motors, Ford, Honda, Mazda, Nissan, Volkswagen, and Hyundai-Kia. *See* CAMP, VSC5, “EE Requirements and Specifications Supporting SCMS Software Release 1.2.2,” under USDOT Cooperative Agreement No. DTNH22-14-H-00449/0003, November 2016. The Vehicle Safety Communications 5 report provides a detailed specification for the configuration and operation of a large scale SCMS deployment capable of issuing and maintaining security credentials for all US road vehicles.

57. This SCMS technology was first introduced in a production vehicle by General Motors in the 2017 CTS. This was followed by Volkswagen in 2019. Both of these OEMs have already made the necessary investments into the security infrastructure and technology development needed to produce vehicles with this technology at scale.

**C. Technical Committee and Working Groups Behind These Standards**

58. The SVI collection of standards brings together technologies that were previously developed for use in V2X applications. Individual standards are typically drafted by smaller working groups. Once individual standards are drafted, technical committees coordinate the development, review, and adoption of collections of standards. Technical Committee 204 (TC204), the committee that coordinated the SVI standards, has broad representation from many industries, including technical representatives from the automotive industry.

59. The standardization process followed by TC204 is shown in Figure 3 below (source: <https://v2g-clarity.com/wp-content/uploads/2019/02/standardization-process-iso-1024x530.png>). This process is staged over a long period of time (a minimum of 2 years, often longer) to give all members of the CEN and ISO standards organizations time to review the draft documents and vote in the multiple rounds of ballot initiatives. All technical objections are addressed prior to approval of a new standard. In all cases, the entire committee has ample opportunity to review, comment on, and eventually vote for approval of new standards. This formal development, review, and adoption process ensures transparency and provides ample opportunities for objections or concerns to be raised and addressed prior to the final adoption and publication of a new standard.

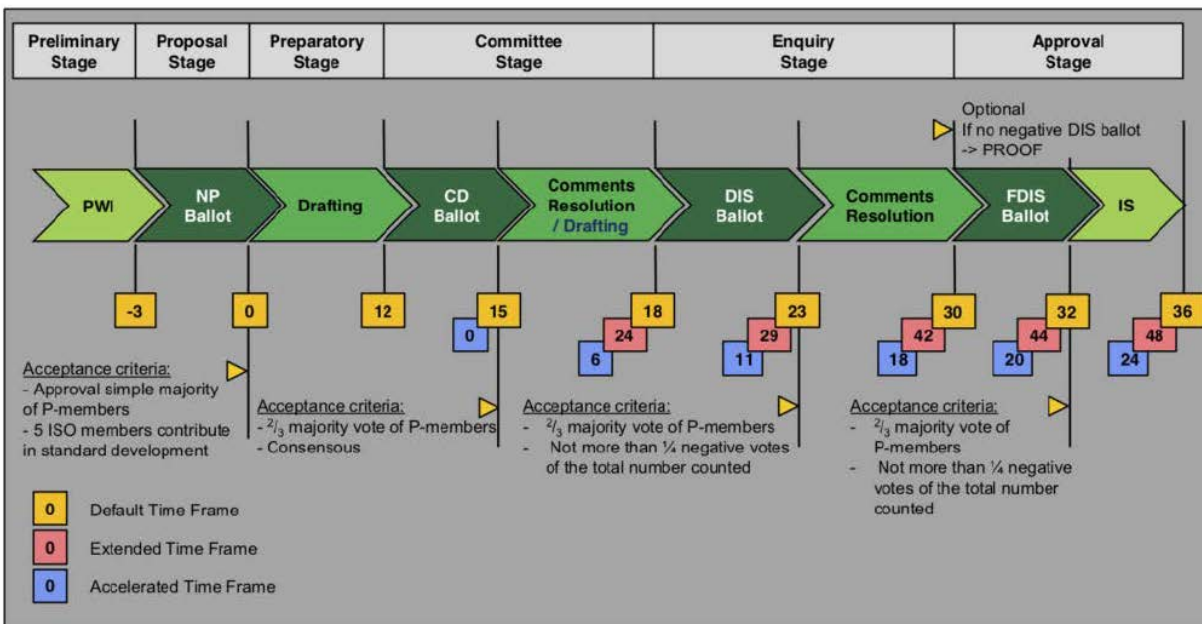


Figure 3: CEN/ISO standard development process.

<https://v2g-clarity.com/wp-content/uploads/2019/02/standardization-process-iso-1024x530.png>

#### D. Maturity of the SVI Standards

60. The individual standards that comprise the SVI architecture are relatively new, but they are built on well-defined, mature technology. The core security and authentication capability behind TS21177 is the IEEE 1609.2 certificate standard that was first published in 2013. The certificate authority (CA) architecture that supports authentication and validation of credentials in the SVI is based on the SCMS that was fully documented and published in 2016.

61. The IEEE 1609.2 certificate technology includes an advanced permissions declaration mechanism that can be used to support role-based access controls. Role-Based Access Control, a best practice in network and computer security, requires that devices and operators have well defined roles and are explicitly authenticated and validated before being granted permission to take a security-sensitive action.

62. At a basic level, this means that different parties can be granted varying levels of permissions based on each party's designated role. A certificate holder's permissions are defined using two fields: (1) a Provider Service Identifier (PSID), which identifies a broad set of application activities which provide a context for the certificate holder's permissions, and (2) a Service Specific Permissions (SSP) field associated with the PSID, which identifies which specific application activities the certificate holder is entitled to carry out within the broad set of activities identified by that PSID. Put simply: the PSID provides a list of possible activities for all parties that hold a certificate, and the SSP identifies which specific activities the individual party can perform based on their designated role, as reflected in the certificate they have. TS21177 provides a generalization of this where additional certificates may be presented to provide additional permissions. For example, a repair tool might initially authenticate to a car using a certificate that is only valid for reading diagnostic data. During the repair process, the same tool may need to write new data to the vehicle as part of a repair. The TS21177 standard describes a mechanism where the tool can send a separate, additional certificate that grants permission for the write operation. In this way, the SVI design can support a "least privilege" model where tools can request only the minimal permissions needed for a specific function, and then escalate or upgrade to other supported permissions only when needed.

63. This advanced permissions-management mechanism allows the certificate authority to grant very specific rights to any participant in a TS21177 transaction. For example, in the case of vehicle service tools, a tool designed to perform a wheel alignment could be granted permission to only update a vehicle's steering calibration (the component that controls wheel alignment). If the alignment tool were to try to write to any other

component in the system other than the steering calibration, the in-vehicle gateway would block the transaction since the tool is not authorized to write to other parts of the vehicle.

64. Similarly, TS21185 builds on standard communication interfaces that have been used in vehicle systems for decades. These include the IEEE 802.11 WiFi interface, IEEE 802.15 Bluetooth standard, and the 3GPP standards for cellular communication. The new TS21185 standard describes how these existing interfaces can be integrated into a coherent system without modifying or changing how they work. For example, TS21185 defines how a repair tool can establish a connection and authenticate to a vehicle using standard WiFi or Bluetooth signals. By referencing the existing wireless connection standards, TS21185 inherits future refinement and new features that may be incorporated into these networking standards.

#### **E. Completeness of the Standards**

65. The SVI architecture, as defined in the three CEN/ISO standards, represents a complete mechanism to establish a secure, authenticated, permissions-based session between a diagnostic tool and a vehicle. The standards further define a mechanism for a vehicle gateway to translate the internal message formats and protocols that are proprietary to the OEM into a common external format that can be shared among service and repair tools. When paired with the necessary hardware, the CEN/ISO standards represent a complete, interoperable solution. (The SVI standards do not prescribe the particular hardware solution that needs to be implemented, so long as it is capable of meeting the standards' requirements. Some potential hardware solutions are discussed by expert Craig Smith.)

66. The standards build on the SCMS certificate management architecture that has been promoted by the DOT for use in V2X applications. This mature, extensively documented solution has provisions for setting up special-purpose Enrollment Certificate Authorities

(ECAs) that can be used to grant specific permissions to individual tools and in-vehicle ECUs. One of the benefits of the SCMS architecture is that these operations can be completely independent of the OEMs and yet ensure security and integrity. The trust in the system is based on a set of certificate issuance policies that are ultimately under the control of a representative group of stakeholders who manage the SCMS Root CA. The SCMS Manager is an authority that can authorize the establishment of new certificate policies and the establishment of new CA types for special purposes, such as issuing credentials for new tools. Rather than attempting to define and create a competing model for each OEM, the SVI architecture relies on this existing infrastructure.

67. Further, the TS21177 specification is based on the most recent, extensively studied, highly trusted TLS 1.3 protocol. (TLS 1.3 is the secure session technology currently recommended for use in all secure internet sessions, such as banking and healthcare transactions conducted using a modern web browser.) In fact, the TS21177 session establishment mechanism inherits the negotiation mechanism that is built into TLS to ensure that both the vehicle and a scan tool can be updated to use future, even more secure versions of the TLS protocol without requiring any changes to the TS21177 standard.

#### **F. Support for Established Security Practices and Safety Mechanisms**

68. The SVI architecture provides a standard mechanism for a diagnostic and repair tool to establish a secure session with a vehicle, as well as an interoperable language and vocabulary for communication between the tool and the car. This enables a secure gateway device (which many newer vehicles are already equipped with) to process the advanced permissions built into the certificate-based PSID/SSP mechanism to enforce a local policy that is appropriate to the individual vehicle. In this instance, a local policy is a specific set of

policy rules implemented in the software developed by an OEM to control their vehicle. The precise method of implementing the SVI standards is left to the discretion of each OEM to make informed decisions based on best practices and their existing safety mechanisms.

69. Many in-vehicle systems today have built-in safety checks, often referred to as “rationality controls,” that validate the state of the vehicle before permitting certain diagnostic or repair procedures. For example, certain calibration procedures require that the vehicle be stationary. This requirement is often enforced at multiple points in the vehicle to ensure that even if one module were compromised, the overall safety of the driver and occupants is protected. The SVI architecture does not require a change to this policy since it only prescribes the standard for interfacing with external devices, not the vehicle’s internal architecture or functions. The same type of defense-in-depth and validation mechanisms that OEMs have in place today can still be applied. The standards that define SVI only require that when the proper conditions are met and an authorized, validated tool presents a request, the vehicle will grant that request using the same internal controls that it would apply if a proprietary OEM command had been issued.

70. Similarly, the SVI architecture does not require that all implementations utilize a common software or hardware implementation. In network security, the principle of diversity recommends that independent implementations of common algorithms should be encouraged. This ensures that a flaw in a single implementation has a limited impact on a broader fleet or network. The adoption of common, open standards such as SVI greatly encourages and facilitates diverse implementations. While all implementation variations must agree on common terminology and protocols, it is possible for many different teams to create their own software and hardware gateway implementations. It is important to note that the

diversity discussed here refers to different implementations of the same algorithm or protocol, not the adoption of secret algorithms where the security value depends entirely in the obscurity of the design.

71. The reliable enforcement of certificate policy, including expiration periods and the interpretation of trusted time, are all accounted for in the SCMS architecture. The association between SCMS and V2V collision avoidance allows for vehicles to accept GPS signals as a time reference. The SCMS security policy defines mechanisms to detect and limit the potential impact of malicious or fake GPS signals from interfering with the in-vehicle time reference.

72. There is also a malicious behavior detection and reporting mechanism built-in to the SCMS infrastructure to account for the potential actions of misconfigured or threatening devices in the network. An extensive revocation mechanism along with a practical way to handle relatively short certificate validity periods ensure that systems which rely on the SVI are resilient to a broad spectrum of threats.

#### **G. Consumer Consent and Governance**

73. In order for the certificates issued by any CA to be trusted, they need to follow a well- defined and commonly understood governance model that regulates the policies and procedures used to review requests for new certificates. Governance within the SVI architecture is inherited from the SCMS certificate management policies, which is ultimately under the control of a representative group of industry stakeholders who participate in the SCMS Manager role. Authorization of specific repair shops for a particular role is handled in the SVI design at the level of trust and certificate-based permissions. This means that

individual repair shops are assigned a particular role and certificate permissions when they register for a certificate.

74. Because the SVI standards do not require one hardware or software implementation, there are multiple methods OEMs could implement to present vehicle owners with the ability to access their mechanical data necessary for diagnostic, repair, or maintenance, and to grant access to a specific repair shops to access that data for a particular repair job. For vehicles equipped with telematics systems, Section 3 of the 2020 Right to Repair Law requires the platform that can securely communicate all mechanical data emanating directly from the vehicle to be “directly accessible by the owner of the vehicle *through a mobile-based application . . .*.” The type of mobile-based application for owner selections is not defined by SVI or the 2020 Right to Repair Law. The mobile-based application could, for example, be implemented as an in-dashboard display, or as part of a software application an OEM can offer to accompany a vehicle. If an OEM chose to provide a mobile-based application to accompany a vehicle, the OEM could provide software that extracts data usage details from the certificate policy presented by a repair shop and then enforces owner-selected choices about where and how their data will be used. The SVI standards do not dictate how this will be done, so the technology enables many possible implementations. Two possible implementations include a mobile application that checks a repair shop’s policy or an established baseline standard policy. The precise implementation details are left as areas for OEMs to differentiate their offerings and show their interest in supporting the vehicle owner’s choice.

## **H. Deployment and Support Cost and Benefits**

75. There is significant cost involved in establishing a new CA infrastructure. The cost to implement the telematics infrastructure (the PKI and associated services that make it possible for repair tools to securely connect to cars) needed to support the diagnosis and repair of vehicles would be shared among all participants, including OEMs, tool vendors, repair shops, and ultimately vehicle owners. Given the close relationship between the SVI architecture and the broader V2X infrastructure, the cost of technology and services specific to vehicle diagnostic and repair, which would be paid for by OEMs and repair tool vendors, would be greatly reduced under this approach. The certificate management function provided by the SCMS will be shared among a multitude of demanding security functions including collision avoidance, roadside infrastructure authorization, emergency vehicle alert capabilities, road hazard warning, and likely additional use cases over time.

76. In addition, implementation of the SVI standards may accrue benefits for OEMs and dealerships in ways that they may not appreciate. For example, the benefits of a secure and interoperable interface to diagnose and repair vehicles would be shared among all participants in the ecosystem. The immediate beneficiaries are the independent repair shops and tool vendors in that this will put them on equal terms with the OEM's captive and preferred dealerships and repair services. However, those dealerships would also gain access to the same common functionality with the benefit of common tools and streamlined authentication and access across all makes and models of cars. Similarly, state operated vehicle inspection equipment and emissions test systems may adopt the same mechanisms to reduce cost and complexity in working with a multitude of vehicle types over time.

77. With a common interface to their vehicles, the OEMs will have the freedom to develop proprietary internal architectures and protocols that are fully independent of the common, external interface. They could rely on the SCMS Manager to set and enforce data access rights policies to protect vehicle owners, the direct customer of the OEMs. They may also reap the benefit of the decades of investment that OEMs have put into the V2X safety and interoperability standards and the certificate infrastructure through expanded use and shared cost of deploying and supporting this new critical road-use infrastructure.

78. OEMs have the option of deciding how to design their own in-vehicle systems. There may be some designs where there is a significant amount of shared hardware and software resources between the V2V collision avoidance technology and the SVI in-vehicle gateway. This approach would reduce the amount of additional hardware needed in the vehicle to support these functions that share many common interfaces and mechanisms. However, some OEMs may choose to take a more modular approach where the SVI gateway would be completely independent of other V2V and V2I interfaces. In either case, the technology expertise and certificate issuance infrastructure would still be shared among all of these functions within the OEM's development and IT team.

#### **I. Development of a Common Data Dictionary**

79. The TS21185 specification provides a mechanism to establish a common "data dictionary" that can translate between proprietary internal messages and protocols used in a specific vehicle and a common set of commands and data representations used by SVI compliant tools. This is a benefit that protects OEM intellectual property and gives them full control over the design and architecture of the in-vehicle network. However, the SVI standards do not define how this common data dictionary will be created or maintained.

80. Today, the translation function is distributed and performed within every after-market scan tool. The information needed to interpret vehicle-specific message formats is managed by groups such as the Equipment and Tool Institute (ETI), which shares this information with tool vendors. It is likely that under the SVI, an organization such as ETI would continue to play a role in defining the standard language and vocabulary that vehicles would use when connecting to after-market tools and services.

81. Since the SVI standards do not mandate how the data dictionary must be maintained, depending on the platform the OEMs choose to implement the SVI standards may make the translation function more secure than it currently is. If the OEMs decide to change their vehicle network architecture to provide access to their vehicles' mechanical data telematically, each OEM could choose to implement the proper translation within their own proprietary gateway device. Under this approach, the OEMs would no longer have to share their internal vehicle network details with the tool vendors—by adopting a common communication format, OEMs would be free to design their own proprietary internal network architecture, provided that they maintain the proper translation functions in the gateway to translate for access by independent, SVI compliant systems.

82. Note that OEMs could optionally implement this functionality as a plug-in module that can be added to a car after it is manufactured. A common way to do this is through the standard J-1962 port already present on all vehicles sold in the US. A brand-specific dongle could apply the same type of data normalization as a built-in system. Similarly, OEMs could collaborate with one or more third party vendors to create after-market devices that apply this level of vehicle-specific data translation.

**J. Conclusion – SVI Provides a Viable Approach for Complying with Section 3**

83. The previous sections have reviewed the history and content of the three international standards that make up SVI architecture. These standards all build on existing technologies, many of which are already adopted in the automotive industry. The process used to create these standards was transparent and open for participation by all of the leading vehicle manufacturers in addition to tool vendors and other interest groups. This collection of standards constitutes a system that fully supports the requirements of Section 3 of the 2020 Right to Repair Law. While the SVI approach is certainly not the only way to assemble a compliant solution, it certainly represents a viable solution that would protect the safety and cybersecurity of vehicles.

**V. Conclusion**

84. I have evaluated the technical options available for compliance with Sections 2 and 3 of the 2020 Right to Repair Law. I conclude that a PKI-based authentication approach is a viable way to achieve compliance with Section 2 which requires that access be granted by an entity that is unaffiliated with any one OEM. The ability for independent CAs to issue credentials clearly satisfies this requirement. Section 3 requires direct access to vehicle systems and a common method of communicating between repair tools and vehicles. The SVI approach provides a detailed, documented, and standards-compliant way to deliver this capability. The combination of these approaches represents a technically sound way to deploy compliant vehicles without compromising driver safety or vehicle cybersecurity.

I declare under the penalty of perjury that the foregoing is true and accurate, this 26<sup>TH</sup>  
day of May 2021.

  
Brian Romansky

# **Exhibit 520**

# B r i a n R o m a n s k y

brian@romansky.com

22 Silvermine Lane, Monroe, CT 06468

203-521-6072

## **Chief Innovation Officer**

### **Owl Cyber Defense, July 2018 - Present**

Owl Cyber Defense is a leading manufacture of network security appliances that implement hardware-enforced policy enforcement for network traffic. As Chief Innovation Officer I am responsible for new product innovation and growth in new markets.

- Launching a new line of embedded FPGA-enabled network security solutions.
- Launching a new line of cloud-edge gateway appliances for critical infrastructure applications.
- Define the future technology strategy and investment priorities needed to support continued growth and competitive differentiation.
- Member of the core management team that manages all aspects of the business.
- Report to the CEO.

## **Senior Director, Strategic Technology and V2X Product Manager**

### **ESCRYPT Canada, April 2017 – June 2018**

ESCRYPT Canada is a division of Robert Bosch GmbH which develops advanced security solutions. The Canadian office provides all new product development in North America for the division. As the Senior Director of Strategic Technology I am responsible for defining the technology strategy and working directly with the management team to execute against that plan and establishing a beachhead in new markets. As Product Manager for V2X solutions, I am directly accountable for defining a new connected vehicle security platform and leading the development, marketing and sales teams to deliver on an aggressive revenue target in a rapidly evolving market. Responsible for defining the technology strategy for North American development of security solutions with a regional target to grow revenue by \$10M over 3 years.

- Defined the technology priorities for entry into the Smart City and IoT markets.
- Product Manager responsible for connected vehicle security solutions including in-vehicle embedded software and back-office certificate management infrastructure.
- Launched a new Intrusion Detection product for identifying and tracking automotive intrusion events. Presented and demonstrated this solution to global automotive manufacturers.
- Accountable for managing the North American patent portfolio and IP strategy.
- Secured and managed government contracts and matching funds in excess of \$500K.
- Reporting to the General Manager, North America.

## **Vice President, Strategic Technology**

### **TrustPoint Innovation, November 2015 – March 2017**

TrustPoint Innovation was a technology startup with expertise in Elliptic Curve Public Key Cryptography. As VP of Strategic Technology, I developed the company's product development and patent strategy. I also acted as a direct consultant and subject matter expert on connected-vehicle technology for the USDOT and Transport Canada. TrustPoint Innovation was acquired by ESCRYPT in March, 2017. I was identified as a key employee in that transaction.

- Implemented a product strategy focused on a connected vehicle security platform.
- Defined product differentiators and market entry strategy for two connected vehicle products.
- Managed the development team that created the technical implementation and first demonstration platform, presented to leading automotive manufacturers and suppliers.
- Delivered consulting services as subject matter expert and technical adviser to the USDOT and Transport Canada for connected-vehicle security infrastructure. Author of multiple sections of the USDOT Security Credential Management System (SCMS) 1.2 specification.
- Secured and managed government contracts and matching funds in excess of \$400K.
- Reported to the CEO.

**Senior Director, New Business Opportunities**  
**Pitney Bowes, November 2008 – October 2015**

The New Business Opportunities (NBO) program was a new business incubator focused on identifying and supporting growth opportunities within the existing business units. I was invited to re-join Pitney Bowes specifically to launch and manage the NBO program. I created and managed a portfolio of projects and reported results directly to the CEO and business unit leadership on growth opportunities. I was also directly responsible for the launch of a spin-out company that was focused on leveraging advanced security technology in the health care market. Created and managed the New Business Opportunities program, an internal incubator that launched new businesses which today account for over \$150M in annual revenue.

- Introduced market-driven, client-focused metrics and hypothesis testing practices for innovation.
- Launched SecLingua, a health care spin-out focused on applying proprietary security technology to deliver advanced connected medical device security. Raised \$0.5M in seed funding and delivered a working prototype, used with live patent data at a regional care facility.
- Reported to the VP of Corporate Strategy.

**Vice President, Technology & Strategy**  
**SyferLock Technology, February 2008 – October 2008**

SyferLock was a technology startup company focused on a innovative user authentication technology to augment conventional passwords. As VP of Technology & Strategy I was responsible for near-term product definition and market entry approach as well as long-term technology strategy for advanced authentication solutions.

- Defined and launched an SSL VPN authentication product and managed the launch of a Windows login client. These products produced the company's first revenue.
- Developed key technical and marketing partnership relationships to expand the company's technical capabilities and market reach.
- Worked directly with clients, defined requirements, designed and delivered custom solutions.
- Reported to the CEO.

**Sr. Director, Business Development and Strategy**  
**Pitney Bowes Management Services, January 2007 - February 2008**

Pitney Bowes Management Services (PBMS) was a \$1B division of Pitney Bowes, focused on delivering on-site managed services. I was invited to join the division to support the development of a growth strategy focused on document management solutions.

- Defined and launched a suite of document management services for the insurance and financial services vertical markets. Solutions focused on incoming document processing.
- Created a marketing program and sales training material that bridged existing capabilities and facilitated entry into higher-value services in the insurance and financial markets.
- Participated directly in the identification and evaluation of business acquisitions opportunities.
- Authored a strategic plan and business model for document management solutions for federal government applications, focusing on expediting Freedom of Information Act (FOIA) processing.
- Member of the Strategic Marketing team, reported to the VP of Marketing.

**Director, Concept Studio**  
**Pitney Bowes, Advanced Concepts & Technology, August 2000 – January 2007**

The Concept Studio was an innovation function within the R&D labs at Pitney Bowes. I launched, staffed, and managed this user-centered design function with an emphasis on developing concepts for targeted growth in strategic markets.

- Assembled and managed a multi-disciplinary team of 10 engineers, designers, workplace anthropologists, and strategic planners who worked in small, teams to serve business unit clients.
- Managed a pipeline of opportunities with an aggregate value of \$100M in recurring revenue.
- Engaged directly with business unit leaders to identify and focus strategic opportunities.
- Selected as a member of the Global Integrated Strategy Team, a task group that developed a long-term company-wide growth strategy. Reported interim results and the final proposal to the CEO and executive management team.

- Member of the R&D management team, reporting to the VP of R&D.

### **Engineer / Sr. Engineer / Manager - Secure Systems**

#### **Pitney Bowes, Advanced Concepts & Technology, September 1993 – August 2000**

The Advanced Concepts & Technology function at Pitney Bowes focused on leading-edge technology and early-stage product concepts to support the global business. As a technical contributor I focused on security-related solutions, developing advanced payment and digital authentication techniques. As a manager, I initiated a new functional organization focused on integrated systems security.

- Implemented advanced machine vision solutions to validate postage on envelopes and packages. This technology drove the adoption and launch of the first digital postage meter, used to secure over \$1B in annual postage funds.
- Created, staffed and managed an IT security research organization responsible for R&D strategy and advanced technology support for systems-level security topics for the global organization.
- Developed and demonstrated an advanced micro-payment technology, secured commitment of \$5M in funding from external investors.
- Managed the FIPS 140 certification submission process for secure software products.
- Reported to the Director of Security Technology.

### **Education and Awards**

- Master of Management – Rensselaer Polytechnic Institute, 1997
- Master of Science, Electrical Engineering – Rensselaer Polytechnic Institute, 1993
- Bachelor of Science, Electrical Engineering – Rensselaer Polytechnic Institute, 1992
- Eta Kappa Nu and Tau Beta Pi, National Engineering Honor Society member
- Inventor on 25 US patents

### **Public Speaking and Presentations**

Frequently invited to speak as a subject matter expert on security technology, connected vehicle systems, and corporate innovation. Selected speaking engagements include:

- Intelligent Transportation Systems World Congress, Copenhagen, 2018
- Intelligent Transportation Systems America, Detroit, 2018
- Embedded World, Nuremberg, 2018
- Intelligent Transportation Systems World Congress, Montreal, 2017
- Embedded Security in Cars (ESCAR-Asia), Tokyo, 2017
- Automotive Parts Manufacturer's Association (APMA), Windsor, 2016
- 4<sup>th</sup> ETSI/IQC Workshop on Quantum-Safe Cryptography, Toronto, 2016
- CloudExpo East, New York, 2016
- Intelligent Cryptographic Module Conference, Montreal, 2016